



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/877,302	06/08/2001	Hovav Shacham	24631.706	9725
7590	11/03/2004			
Brian R. Coleman Perkins Coie LLP P.O. Box 2168 Menlo Park, CA 94026			EXAMINER PARTHASARATHY, PRAMILA	
			ART UNIT 2136	PAPER NUMBER
DATE MAILED: 11/03/2004				

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/877,302	<b>Applicant(s)</b> SHACHAM ET AL.	
	<b>Examiner</b> Pramila Parthasarathy	<b>Art Unit</b> 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 05/09/2003.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-76 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-76 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

1. This action is in response to the communication filed on 05/09/2003. Claims 1 – 76 were received for consideration. No preliminary amendments to the claims were filed on. Claims 1 – 76 are currently being considered.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1, 5 – 9, 13 – 17, 21 – 25, 29 – 32, 46, 50 – 52, 56, 60 – 63, 75 and 76 are rejected under 35 U.S.C. 102(b) as being anticipated by Fiat (U.S. Patent Number 4,964,164).

Regarding Claim 1, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), comprising;

combining individually encrypted network security protection handshake messages into a set of encrypted messages wherein each encrypted handshake message is derived using a public key containing an encryption exponent (Column 1

line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43 and Column 5 lines 20 – 56);

determining a root node of a binary tree comprising leaf nodes corresponding to each encryption exponent (Column 3 lines 63 – Column 4 line 43 and Column 5 lines 20 – 50);

calculating a product of the encrypted messages (Column 4 lines 12 – 43 and Column 5 lines 20 – 50);

extracting at least one root from the product of the encrypted messages (Column 4 lines 12 – 58 and Column 5 lines 20 – 56); and

decrypting the encrypted messages by expressing the at least one root as at least one promise and evaluating the at least one promise at the leaf nodes decreasing the number of modular inversions wherein efficiency of the decryption is increased (Column 1 line 63 – Column 2 line 11 and Column 6 line 53 – Column 7 line 4).

Regarding Claim 9, Fiat teaches and describes a method for improving secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), comprising;

combining individually encrypted network security protection handshake messages into a set of encrypted messages wherein each encrypted handshake message is derived using a public key containing an encryption exponent (Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43 and Column 5 lines 20 – 56);

determining a root node of a binary tree comprising leaf nodes corresponding to the encryption exponent of each encrypted message (Column 3 lines 63 – Column 4 line 43 and Column 5 lines 20 – 50);

calculating a product of the encrypted messages (Column 4 lines 12 – 43 and Column 5 lines 20 – 50);

extracting at least one root from the product of the encrypted messages (Column 4 lines 12 – 58 and Column 5 lines 20 – 56); and

decrypting the encrypted messages by evaluating at least one individual leaf node by multiplying an inversion of the total product of leaf nodes with a partial product of the leaf nodes to produce an inversion of the at least one individual leaf node wherein efficiency of the decryption is increased (Column 1 line 63 – Column 2 line 11 and Column 6 line 53 – Column 7 line 4).

Regarding Claim 17, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), comprising;

combining individually encrypted network security protection handshake messages into a set of encrypted messages wherein each encrypted handshake message is derived using a public key containing an encryption exponent (Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43 and Column 5 lines 20 – 56);

determining a root node of a binary tree comprising leaf nodes corresponding to the encryption exponent of each encrypted message (Column 3 lines 63 – Column 4 line 43 and Column 5 lines 20 – 50);

calculating a product of the encrypted messages (Column 4 lines 12 – 43 and Column 5 lines 20 – 50);

extracting at least one root from the product of the encrypted messages (Column 4 lines 12 – 58 and Column 5 lines 20 – 56);

decrypting the encrypted messages by minimizing the disparity between the sizes of the encryption exponents of the public keys, wherein efficiency of the secure communications is increased (Column 1 line 63 – Column 2 line 11 and Column 6 line 53 – Column 7 line 4).

Regarding Claim 25, Fiat teaches and describes a method for improving secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), comprising:

combining individually encrypted network security protection handshake into a set of encrypted messages wherein each encrypted handshake message is derived using a public key containing an encryption exponent (Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43 and Column 5 lines 20 – 56);

determining a root node of a binary tree comprising leaf nodes corresponding to each encryption exponent by using a plurality of separate parallel batch trees finding the

Art Unit: 2136

root node of each tree and combining the final answers (Column 3 lines 63 – Column 4 line 43 and Column 5 lines 20 – 50);

calculating a product of the encrypted messages (Column 4 lines 12 – 43 and Column 5 lines 20 – 50);

extracting at least one root from the product of the encrypted messages (Column 4 lines 12 – 58 and Column 5 lines 20 – 56); and

decrypting the encrypted messages by expressing the at least one root as at least one promise and evaluating the at least one promise at the leaf nodes producing a reduced number of modular inversions wherein efficiency of establishing secure communications is increased (Column 1 line 63 – Column 2 line 11 and Column 6 line 53 – Column 7 line 4).

Regarding Claim 32, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), comprising;

combining individually encrypted network security protection messages into a set of encrypted messages, wherein each encrypted handshake message is derived using a public key containing an encryption exponent (Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43 and Column 5 lines 20 – 56);

determining a root node of a binary tree comprising leaf nodes corresponding to each encrypted messages encryption exponent (Column 3 lines 63 – Column 4 line 43 and Column 5 lines 20 – 50);

calculating a product of the encrypted messages (Column 4 lines 12 – 43 and Column 5 lines 20 – 50);

minimizing the disparity among the sizes of the encryption exponents of the public keys within the set (Column 2 line 67 – Column 3 line 20 and Column 4 lines 1 – 11);

extracting at least one root from the product of the encrypted messages (Column 4 lines 12 – 58 and Column 5 lines 20 – 56); and

decrypting the encrypted messages by evaluating the at least one leaf node by multiplying an inversion of a total product of the leaf nodes with a partial product of the leaf nodes to produce the inversion of the at least one leaf node wherein efficiency of establishing secure network communications is increased (Column 1 line 63 – Column 2 line 11 and Column 6 line 53 – Column 7 line 4).

Regarding Claim 46, Fiat teaches and describes a method for batch decryption in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), comprising:

combining a plurality of encrypted messages into a plurality of batches, wherein each encrypted message includes a public / private key pair, each public key comprising an encryption exponent (Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43 and Column 5 lines 20 – 56);

scheduling the batches of encrypted messages using a plurality of criteria selected from a group including maximum throughput, minimum turnaround-time,



minimum turnaround-time variance, and server load considerations, wherein the efficiency of establishing secure communications is enhanced (Column 3 lines 34 – 56); and

replacing at least one inversion of at least one batch decryption operation with a single inversion and a plurality of multiplication operations, wherein the speed of the decryption is significantly improved (Column 1 line 63 – Column 2 line 11 and Column 6 line 53 – Column 7 line 4).

Regarding Claim 52, Fiat teaches and describes 52. A method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), comprising;

combining individually encrypted network security protection handshake messages into a set of encrypted handshake messages wherein each encrypted message is derived using a public key comprising an encryption exponent (Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43 and Column 5 lines 20 – 56);

determining a root node of a binary tree containing leaf nodes corresponding to each encrypted message encryption exponent by using a plurality of separate parallel batch trees finding the root node of each tree and combining the final answers (Column 3 lines 63 – Column 4 line 43 and Column 5 lines 20 – 50);

minimizing the disparity between the sizes of the encryption exponents of the public keys within the set; using simultaneous multiple exponentiation such that the

encryption exponents are combined to reduce the number of exponentiations (Column 3 lines 34 – 56);

calculating a product of the encrypted messages (Column 4 lines 12 – 43 and Column 5 lines 20 – 50);

extracting at least one root from the product of the encrypted messages (Column 4 lines 12 – 58 and Column 5 lines 20 – 56); and

decrypting the encrypted messages by expressing the at least one root as at least one promise and evaluating the at least one promise at the leaf nodes, and multiplying an inversion of a total product of the leaf nodes with a partial product of the leaf nodes decreasing the number of modular inversions by producing an inversion of the leaf node wherein efficiency of secure communications is increased (Column 1 line 63 – Column 2 line 11 and Column 6 line 53 – Column 7 line 4).

Regarding Claim 56, Fiat teaches and describes a method for performing batch decryption in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), comprising:

receiving a plurality of encrypted messages generated using a plurality of public keys, wherein the plurality of public keys share a common modulus (Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43 and Column 5 lines 20 – 56);

forming a binary tree using leaf nodes corresponding to the plurality of public keys; placing each of the plurality of encrypted messages in a leaf node having

a corresponding public key (Column 4 lines 59 – 64);

percolating the plurality of encrypted messages up the binary tree to form a root node including a product of the encrypted messages, extracting at least one root from the product of the encrypted messages by forming an exponentiation product in the root node (Column 4 lines 12 – 58 and Column 5 lines 20 – 56);

expressing the at least one root using at least one promise that includes at least one alternative representation of at least one arithmetic function of the at least one root; percolating the at least one root down the binary tree using the at least one promise (Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43 and Column 5 lines 20 – 56); and

decrypting the plurality of encrypted messages by evaluating the at least one promise at the leaf nodes, wherein efficiency of the decryption is increased by reducing a number of modular inversions and a number of root extractions (Column 1 line 63 – Column 2 line 11 and Column 6 line 53 – Column 7 line 4).

Regarding Claim 75, Fiat teaches and describes a computer-readable medium, comprising executable instructions for establishing secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), which, when executed in a processing system, causes the system to:

combine individually encrypted network security protection handshake messages into a set of encrypted messages wherein each encrypted handshake message is

Art Unit: 2136

derived using a public key comprising an encryption exponent (Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43 and Column 5 lines 20 – 56);

determine a root node of a binary tree containing leaf nodes corresponding to each encrypted messages encryption exponent by using a plurality of separate parallel batch trees to find the root node of each tree and combine the final answers (Column 3 lines 63 – Column 4 line 43 and Column 5 lines 20 – 50);

minimize the disparity between the sizes of the encryption exponents of the public keys within the set; combine the encryption exponents using simultaneous multiple exponentiation such that the number of exponentiations is reduced (Column 3 lines 34 – 56);

calculate a product of the encrypted messages (Column 4 lines 12 – 43 and Column 5 lines 20 – 50);

extract at least one root from the product of the encrypted messages (Column 4 lines 12 – 58 and Column 5 lines 20 – 56); and

decrypt the encrypted messages by expressing the at least one root as at least one promise and evaluating the at least one promise at the leaf nodes, multiplying an inversion of a total product of the leaf nodes with a partial product of the leaf nodes producing an inversion of the leaf node and decreasing the number of modular inversions, wherein efficiency of establishing secure communications is increased (Column 1 line 63 – Column 2 line 11 and Column 6 line 53 – Column 7 line 4).

Regarding Claim 76, Fiat teaches and describes an electromagnetic medium, comprising executable instructions for establishing secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), which, when executed in a processing system, causes the system to;

combine individually encrypted secure network handshake messages into a set of encrypted handshake messages wherein each encrypted handshake message is derived using a public key comprising an encryption exponent (Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43 and Column 5 lines 20 – 56);

determine a root node of a binary tree containing leaf nodes corresponding to each encrypted messages encryption exponent by using a plurality of separate parallel batch trees to find the root node of each tree and combine the final answers (Column 3 lines 63 – Column 4 line 43 and Column 5 lines 20 – 50);

minimize the disparity between the sizes of the encryption exponents of the public keys within the set; combine the encryption exponents using simultaneous multiple exponentiation such that the number of exponentiations is reduced (Column 3 lines 34 – 56);

calculate a product of the encrypted messages (Column 4 lines 12 – 43 and Column 5 lines 20 – 50);

extract at least one root from the product of the encrypted messages (Column 4 lines 12 – 58 and Column 5 lines 20 – 56); and

decrypt the encrypted messages by expressing the at least one root as at

least one promise and evaluating the at least one promise at the leaf nodes, multiplying an inversion of a total product of the leaf nodes with a partial product of the leaf nodes producing an inversion of the leaf node, and decreasing the number of modular inversions wherein efficiency of establishing secure communications is increased (Column 1 line 63 – Column 2 line 11 and Column 6 line 53 – Column 7 line 4).

Claims 5, 24 and 30 are rejected as applied above in rejecting claims 1, 17 and 25. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17) wherein evaluating the at least one promise includes multiplying an inversion of a total product of the leaf nodes with a partial product of the leaf nodes to produce the inversion of an individual leaf node (Column 4 line 59 – Column 5 line 17).

Claims 6, 13 and 31 are rejected as applied above in rejecting claims 1, 9 and 25. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), further comprising minimizing the disparity among the sizes of the encryption exponents of the public keys within the set (Column 4 line 59 – Column 5 line 17 and Column 7 lines 5 – 17).

Claims 7, 14, 21 and 50 are rejected as applied above in rejecting claims 1, 9, 17 and 46. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17) wherein determining includes using a plurality of separate, parallel batch trees finding the root node of each tree and combining the final answers (Column 5 line 5 – 49).

Claims 8, 15, 22 and 29 are rejected as applied above in rejecting claims 1, 9, 17 and 25. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), wherein decrypting includes simultaneous multiple exponentiation such that the encryption exponents are combined to reduce the number of exponentiations (Column 4 line 59 – Column 5 line 17 and Column 6 line 53 – Column 7 line 4).

Claims 16 and 23 are rejected as applied above in rejecting claims 9 and 17. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), wherein decrypting includes expressing the at least one root as at least one promise and evaluation the at least one promise at the leaf nodes decreasing the number of modular inversions (Column 4 line 59 – Column 5 line 17).

Claim 51 is rejected as applied above in rejecting claim 46. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), wherein combining includes selecting the encrypted messages for the batches by balancing the encryption exponent (Column 4 line 45 – Column 5 line 10).

Claim 60 is rejected as applied above in rejecting claim 56. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), wherein evaluating the at least one promise uses batched division to calculate a plurality of inverses for the plurality of leaf nodes using a single modular inversion, wherein the single modular inversion is multiplied with a partial product at each leaf node to produce a corresponding inverse for the leaf node.

Claim 61 is rejected as applied above in rejecting claim 56. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), further comprising: reducing each of the plurality of encrypted messages modulo  $p$  and  $q$ ; generating two parallel batch trees modulo  $p$  and  $q$ ; and batching in each of the two parallel batch trees modulo  $p$  and  $q$  (Column 5 line 5 – 49).



Claim 62 is rejected as applied above in rejecting claim 56. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), wherein the percolating includes balanced exponents (Column 4 line 45 – Column 5 line 10).

Claim 63 is rejected as applied above in rejecting claim 56. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), wherein the percolating includes simultaneous multiple exponentiation (Column 4 line 59 – Column 5 line 17 and Column 6 line 53 – Column 7 line 4).

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 2, 10, 18, 26, 33, 36, 37, 40 – 45, 47, 53, 57, 64 – 67 and 70 – 74 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fiat (U.S. Patent Number

4,964,164, hereinafter "Fiat") in view of Corella (U.S. Patent Number 6,763,459, hereinafter "Corella").

Regarding Claim 36, Fiat teaches and describes a method for secure communications in a computer network (Fiat Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17). Fiat does not explicitly disclose a computer network comprising coupling a client to a web server, sending a client hello message to the web server, generating a public / private key pair at the web server, wherein the public key contains an encryption exponent; and responding to the client with a server hello message comprising the public key. However, Corella discloses a PKI infrastructure including an online registration authority, an off-line credential server, and a verifier (Corella Summary; Fig. 12 – 16 and Column 5 line 6 – Column 15 line 24) wherein, the credential server is linked by one or more computer networks and a network connections comprising:

coupling a client to a web server (Corella Column 6 lines 36 – 50; Column 13 lines 19 – 24 and Column 14 lines 25 – 33);

sending a client hello message to the web server (Corella Column 8 lines 16 – 22 and Column 10 lines 41 – 48);

generating a public / private key pair at the web server, wherein the public key contains an encryption exponent responding to the client with a server hello message comprising the public key (Corella Column 6 line 51 – Column 7 line 23 and Column 11 lines 32 – 37);

encrypting a random handshake message at the client using the public

key (Corella Column 13 lines 51 – 54);

sending the encrypted handshake message to a batch-decryption server (Corella Column 13 lines 60 – 65);

batching handshake messages on a batch-decryption server according to the public key such that the disparity between the sizes of the encryption exponents of the public key is minimized (Fiat Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43 and Column 5 lines 20 – 56);

separating the batch's  $e^{\text{th}}$  root in a downward-percolation phase into constituent decrypted messages, wherein internal inversions are converted to modular divisions increasing efficiency by producing a reduced number of modular inversions (Fiat Column 4 lines 12 – 58 and Column 5 lines 20 – 56);

scheduling the batch-decryption server based on server-load considerations (Fiat Column 7 lines 5 – 25);

decrypting the handshake messages using at least one alternate expression of at least one arithmetic function of at least one batch's  $e^{\text{th}}$  root, and sending the decrypted message to the web server (Fiat Column 1 line 63 – Column 2 line 11 and Column 6 line 53 – Column 7 line 4).

Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method to batching handshake messages for encrypting and decrypting as taught by Fiat in the combined system to provide secure communication with a client coupling to a web server and generating a public/private key pair at the web server as taught by Corella. The modification would be

obvious because of one of ordinary skill in the art would be motivated to batch signature/encryption processing or any public key encryption scheme from clients for fast method for extracting multiple roots multiple roots and a fast method for computing products in a client/server environment.

Regarding Claim 64, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17). Fiat discloses generating a Rivest-Shamir-Adleman ("RSA") public / private key pair and combining individually encrypted messages to form a batch (Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43 and Column 5 lines 20 – 56); decrypting the batch of messages using the RSA private keys to determine R, wherein the efficiency of the decryption is enhanced by replacing at least one inversion with at least one multiplication (Column 1 line 63 – Column 2 line 11 and Column 6 line 53 – Column 7 line 4). Fiat does not disclose generating a Rivest-Shamir-Adleman ("RSA") public / private key pair at a web server; coupling a client to the web server; sending a client hello message to the web server requesting the establishment of a Secure Socket Layer ("SSL"); responding to the client with a server hello message containing the RSA public key; encrypting a random string R, the pre-master secret at the client, using the RSA public key, wherein the resulting cipher-text, C, contains R; sending the encrypted cipher-text message, C, to the web server; combining individually encrypted secure socket layer ("SSL") encrypted cipher-text messages to form a batch and establishing a common session

Art Unit: 2136

key between the web server and the client using R. However, Corella discloses a PKI infrastructure including an online registration authority, an off-line credential server, and a verifier (Corella Summary; Fig. 12 – 16 and Column 5 line 6 – Column 15 line 24) wherein, the credential server is linked by one or more computer networks and a network connections comprising:

- generating a Rivest-Shamir-Adleman (“RSA”) public / private key pair at the web server (Corella Column 6 line 51 – Column 7 line 23 and Column 11 lines 32 – 37);

- coupling a client to a web server (Corella Column 6 lines 36 – 50; Column 13 lines 19 – 24 and Column 14 lines 25 – 33);

- sending a client hello message to the web server requesting the establishment of a Secure Socket Layer (“SSL”) (Corella Column 8 lines 16 – 22 and Column 10 lines 41 – 48);

- encrypting a random string R, the pre-master secret at the client, using the RSA public key wherein the resulting cipher-text, C, contains R (Corella Column 13 lines 51 – 54);

- sending the encrypted cipher-text message to a batch (Corella Column 13 lines 60 – 65); and

- establishing a common session key between the web server and the client using R (Corella Column 13 lines 51 – 65).

Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method to batching handshake messages for encrypting and decrypting as taught by Fiat in the combined system to

provide secure communication with a client coupling to a web server and generating a public/private key pair at the web server as taught by Corella. The modification would be obvious because of one of ordinary skill in the art would be motivated to batch signature/encryption processing or any public key encryption scheme from clients for fast method for extracting multiple roots multiple roots and a fast method for computing products in a client/server environment.

Regarding Claim 66, Fiat teaches and describes a system for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17). Fiat discloses receiving requests for decryption of a plurality of individually encrypted network secure protection messages, aggregates the plurality of individually encrypted messages into at least one batch wherein each encrypted message is derived by using an encryption exponent from an Rivest-shamir-Adleman ("RSA") public / private key pair, forms a binary tree containing leaf nodes corresponding to each encryption exponent, extracts at least one root from a product of the encrypted messages (Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43 and Column 5 lines 20 – 56). Fiat does not disclose at least one batch server coupled among the at least one client processor and the at least one web servers wherein the at least one batch server receives requests for decryption of a plurality of individually encrypted network secure protection handshake messages, aggregates the plurality of individually encrypted handshake messages into at least one batch. However, Corella discloses a PKI infrastructure including an online registration

authority, an off-line credential server, and a verifier (Corella Summary; Fig. 12 – 16 and Column 5 line 6 – Column 15 line 24) wherein, the credential server is linked by one or more computer networks and a network connections comprising:

at least one client processor (Corella Column 6 line 36 – 50; Column 13 lines 19 – 24 and Column 14 lines 25 – 33);

at least one web server (Corella Column 8 lines 16 – 22 and Column 10 lines 41 – 48); and

at least one batch server coupled among the at least one client processor and the at least one web servers wherein the at least one batch server receives requests for decryption of a plurality of individually encrypted network secure protection handshake messages, aggregates the plurality of individually encrypted handshake messages into at least one batch wherein each encrypted message is derived by using an encryption exponent from an Rivest-shamir-Adleman ("RSA") public / private key pair, forms a binary tree containing leaf nodes corresponding to each encryption exponent, extracts at least one root from a product of the encrypted messages (Fiat Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43; Column 5 lines 20 – 56 and Corella Column 6 lines 36 – Column 7 line 23; Column 8 lines 16 – 22; Column 11 lines 32 – 37),

decrypts the encrypted messages by expressing the at least one root as at least one promise and evaluating the at least one promise at the leaf nodes, and multiplies an inversion of a total product of the leaf nodes with a partial product of the leaf nodes producing an inversion of the leaf node decreasing the number of modular inversions,

and responds to the requests for decryption with corresponding plain-text (Fiat Column 1 line 63 – Column 2 line 11 and Column 6 line 53 – Column 7 line 4).

Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method to batching handshake messages for encrypting and decrypting as taught by Fiat in the combined system to provide secure communication with a client coupling to a web server and generating a public/private key pair at the web server as taught by Corella. The modification would be obvious because of one of ordinary skill in the art would be motivated to batch signature/encryption processing or any public key encryption scheme from clients for fast method for extracting multiple roots multiple roots and a fast method for computing products in a client/server environment.

Regarding Claim 71, Fiat teaches and describes a system for secure communications in a computer network (Fiat Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), receives requests for decryption of a plurality of individually encrypted network security protection messages, aggregates the plurality of individually encrypted messages into at least one batch wherein each encrypted message is derived using an encryption exponent from an Rivest-shamir-Adleman ("RSA") public / private key pair, forms a binary tree containing leaf nodes corresponding to each encryption exponent, extracts at least one root from a product of the encrypted messages (Fiat Column 4 lines 12 – 58 and Column 5 lines 20 – 56), decrypts the encrypted messages by expressing the at least one root as at least one



promise and evaluating the at least one promise at the leaf nodes, and multiplies an inversion of a total product of the leaf nodes with a partial product of the leaf nodes producing an inversion of the leaf node decreasing the number of modular inversions, wherein efficiency of secure communications is increased (Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43; Column 5 lines 20 – 56 and Column 6 line 53 – Column 7 line 4). Fiat does not explicitly disclose a client processor coupled among at least one web server, wherein the web server receives requests for decryption of a plurality of individually encrypted network security protection handshake messages.

However, Corella discloses a PKI infrastructure including an online registration authority, an off-line credential server, and a verifier (Corella Summary; Fig. 12 – 16 and Column 5 line 6 – Column 15 line 24) wherein, the credential server is linked by one or more computer networks and a network connections comprising: at least one client processor coupled among at least one web server, wherein the web server receives requests for decryption of a plurality of individually encrypted network security protection handshake messages (Corella Column 6 lines 36 – 50; Column 8 lines 16 – 22; Column 10 lines 41 – 48; Column 13 lines 19 – 24 and Column 14 lines 25 – 33).

Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method to batching handshake messages for encrypting and decrypting as taught by Fiat in the combined system to provide secure communication with a client coupling to a web server and generating a public/private key pair at the web server as taught by Corella. The modification would be

obvious because of one of ordinary skill in the art would be motivated to batch signature/encryption processing or any public key encryption scheme from clients for fast method for extracting multiple roots multiple roots and a fast method for computing products in a client/server environment.

Regarding Claim 72, Fiat teaches and describes a system of scheduling batch decryption in a computer network (Fiat Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), comprising:

using a Rivest-shamir-Adleman ("RSA") decryption algorithm, wherein the at least one batch server links the plurality of client processors to the at least one web server; and a scheduler, wherein during a timed period the scheduler places arriving encrypted messages in a queue forming a batch, wherein the encrypted messages in the queue are decrypted upon completion of the timed period (Fiat Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43; Column 5 lines 20 – 56 and Column 6 line 53 – Column 7 line 4). Fiat does not explicitly disclose a plurality of client processor, at least one web server, at least one batch server coupled among the at least one web server.

However, Corella discloses a PKI infrastructure including an online registration authority, an off-line credential server, and a verifier (Corella Summary; Fig. 12 – 16 and Column 5 line 6 – Column 15 line 24) wherein, the credential server is linked by one or more computer networks and a network connections comprising: at least one client processor coupled among at least one web server, wherein a plurality of client

Art Unit: 2136

processors; at least one web server; at least one batch server coupled among the at least one web server (Corella Column 6 lines 36 – 50; Column 8 lines 16 – 22; Column 10 lines 41 – 48; Column 13 lines 19 – 24 and Column 14 lines 25 – 33).

Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method to batching handshake messages for encrypting and decrypting as taught by Fiat in the combined system to provide secure communication with a client coupling to a web server and generating a public/private key pair at the web server as taught by Corella. The modification would be obvious because of one of ordinary skill in the art would be motivated to batch signature/encryption processing or any public key encryption scheme from clients for fast method for extracting multiple roots multiple roots and a fast method for computing products in a client/server environment.

Regarding Claim 73, Fiat teaches and describes a system for secure network communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), generating a Rivest-Shamir-Adleman ("RSA") public / private key pair and combining individually encrypted messages to form a batch algorithm to decrypt an aggregation of encrypted messages (Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column 4 line 43 and Column 5 lines 20 – 56). Fiat does not explicitly disclose a plurality of client processor, at least one web server, at least one batch server coupled among the at least one web server.

However, Corella discloses a PKI infrastructure including an online registration authority, an off-line credential server, and a verifier (Corella Summary; Fig. 12 – 16 and Column 5 line 6 – Column 15 line 24) comprising at least one batch server coupled among at least one client processor and at least one web server, wherein the at least one batch server uses a Rivest-shamir-Adleman ("RSA") (Corella Column 6 lines 36 – 50; Column 8 lines 16 – 22; Column 10 lines 41 – 48; Column 13 lines 19 – 24 and Column 14 lines 25 – 33).

Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method to batching handshake messages for encrypting and decrypting as taught by Fiat in the combined system to provide secure communication with a client coupling to a web server and generating a public/private key pair at the web server as taught by Corella. The modification would be obvious because of one of ordinary skill in the art would be motivated to batch signature/encryption processing or any public key encryption scheme from clients for fast method for extracting multiple roots multiple roots and a fast method for computing products in a client/server environment.

Regarding Claim 74, Fiat teaches and describes a system for secure computer network communications (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), combines decryption requests messages into at least one batch and decrypts the at least one batch using a Rivest-shamir-Adleman ("RSA") batch decryption algorithm (Column 1 line 25 – Column 2 line 57; Column 3 line 63 – Column

Art Unit: 2136

4 line 43 and Column 5 lines 20 – 56). Fiat does not explicitly disclose the messages of Secure Socket Layer ("SSL"). However, Corella discloses a PKI infrastructure including an online registration authority, an off-line credential server, and a verifier (Corella Summary; Fig. 12 – 16 and Column 5 line 6 – Column 15 line 24) comprising at least one batch server coupled among at least one client processor and at least one web server and the messages of Secure Socket Layer ("SSL"), wherein the at least one batch server uses a Rivest-shamir-Adleman ("RSA") (Corella Column 6 lines 36 – 50; Column 8 lines 16 – 22; Column 10 lines 41 – 48; Column 13 lines 19 – 24 and Column 14 lines 25 – 33).

Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method to batching handshake messages for encrypting and decrypting as taught by Fiat in the combined system to provide secure communication with a client coupling to a web server and generating a public/private key pair at the web server as taught by Corella. The modification would be obvious because of one of ordinary skill in the art would be motivated to batch signature/encryption processing or any public key encryption scheme from clients for fast method for extracting multiple roots multiple roots and a fast method for computing products in a client/server environment.

Claims 2, 10, 18, 26, 33, 37, 47, 53, 57 and 67 are rejected as applied above in rejecting claims 1, 9, 17, 25, 32, 36, 46, 52, 56 and 66. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects

and summary of the invention and Column 3 line 57 – Column 7 line 17). Fiat does not explicitly disclose the secure communications include secure socket layer ("SSL") messages.

However, Corella discloses a PKI infrastructure including an online registration authority, an off-line credential server, and a verifier (Corella Summary; Fig. 12 – 16 and Column 5 line 6 – Column 15 line 24) comprising at least one batch server coupled among at least one client processor and at least one web server wherein the secure communications include Secure Socket Layer ("SSL") (Corella Column 6 lines 36 – 50; Column 8 lines 16 – 22; Column 10 lines 41 – 48; Column 13 lines 19 – 24 and Column 14 lines 25 – 33).

Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method to batching handshake messages for encrypting and decrypting as taught by Fiat in the combined system to provide secure communication with a client coupling to a web server with "SSL" as taught by Corella. The modification would be obvious because of one of ordinary skill in the art would be motivated to batch signature/encryption processing or any public key encryption scheme from clients for fast method for extracting multiple roots multiple roots and a fast method for computing products in a secure client/server environment.

Claim 40 is rejected as applied above in rejecting claim 36. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line

17), wherein batching further comprises an upward-percolation phase that combines individual encrypted messages to form a value,  $v$  wherein  $v$  is the product of the individual encrypted messages raised to the power of  $e/e_1$ ,  $e$  being the product of all individual encryption exponents  $e_1$  (Column 5 line 5 – 40).

Claim 41 is rejected as applied above in rejecting claim 36. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), wherein the value  $v$  is determined by the equation where  $e$  is the product of individual exponentiation exponents,  $v_i$  is the individual encrypted message,  $e_i$  is the individual public key, and  $b$  is the number of encrypted messages in a particular batch (Fig. 1 “message data signals” and Column 5 line 21 – Column 6 line 39).

Claim 42 is rejected as applied above in rejecting claim 36. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), wherein batching further comprises an exponentiation phase that includes the extraction of an  $e^{\text{th}}$  root from the value,  $v$  (Column 5 lines 52 – 54).

Claim 43 is rejected as applied above in rejecting claim 36. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line

17), wherein exponentiation further includes simultaneous multiple exponentiation such that the encryption exponents are combined to reduce the number of exponentiations (Column 4 line 59 – Column 5 line 17 and Column 6 line 53 - Column 7 line 4).

Claim 44 is rejected as applied above in rejecting claim 36. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), wherein exponentiation includes combining a plurality of inversions to form a single modular inversion (Column 4 line 12 – Column 5 line 56).

Claim 45 is rejected as applied above in rejecting claim 36. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), wherein decrypting includes reducing each encrypted batch message into a separate module, using separate parallel batch trees to determine the module, and combining the final answers (Column 5 line 5 – 49)

Claim 65 is rejected as applied above in rejecting claim 36. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), wherein decrypting includes using at least one alternative representation of at least



one arithmetic function to reduce to the number of inversions (Column 4 line 49 – Column 5 line 17 and Column 6 line 53 – Column 7 line 4).

Claim 70 is rejected as applied above in rejecting claim 66. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17), wherein the batch server aggregates the plurality of encrypted messages base on criteria including maximum throughput, minimum turnaround time, and minimum turnaround time variance (Column 1 line 63 – Column 2 line 11 and Column 6 line 53 – Column 7 line 4).

3. Claims 3, 4, 11, 12, 19, 20, 27, 28, 34, 35, 38, 39, 48, 49, 54, 55, 58, 59, 68 and 69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fiat (U.S. Patent Number 4,964,164, hereinafter “Fiat”) in view of Corella (U.S. Patent Number 6,763,459, hereinafter “Corella”) and further in view of Rao et al. (U.S. Patent Number 6,757,823, hereinafter “Rao”).

Claims 3, 4, 11, 12, 19, 20, 27, 28, 34, 35, 38, 39, 48, 49, 54, 55, 58, 59, 68 and 69 are rejected as applied above in rejecting claims 1, 9, 17, 25, 32, 36, 46, 52, 56 and 66. Furthermore, Fiat teaches and describes a method for secure communications in a computer network (Fig. 1; Objects and summary of the invention and Column 3 line 57 – Column 7 line 17). Fiat does not explicitly disclose the secure communications include

transport layer security ("TLS") messages or "IPSec" messages. Corella discloses a PKI infrastructure including an online registration authority, an off-line credential server, and a verifier (Corella Summary; Fig. 12 – 16 and Column 5 line 6 – Column 15 line 24) comprising at least one batch server coupled among at least one client processor and at least one web server wherein the secure communications (Corella Column 6 lines 36 – 50; Column 8 lines 16 – 22; Column 10 lines 41 – 48; Column 13 lines 19 – 24 and Column 14 lines 25 – 33). Even when combined, Fiat and Corella do not teach that the secure communications include transport layer security ("TLS") messages and "IPSec" messages.

However, Rao discloses a method of providing secure connections for network telephony calls, wherein a call signaling channel is secured by using either a Transport Layer Security Protocol ("TLS"), a Secure Sockets Layer ("SSL") or an IP Security Protocol (IPSec) on a secure well known port (Column 1 line 15 – 36).

Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method to batching handshake messages for encrypting and decrypting as taught by Fiat in the combined system to provide secure communication with a client coupling to a web server with "TLS" or "IPSec" as taught by Rao. The modification would be obvious because of one of ordinary skill in the art would be motivated to batch signature/encryption processing or any public key encryption scheme from clients for fast method for extracting multiple roots multiple roots and a fast method for computing products in a secure client/server environment.

4. Any response to this action should be mailed to:


Commissioner of Patents and Trademarks, Washington, D.C. 20231 **or**  
**faxed to:** (703) 872-9306 for all formal communications.

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Fourth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571 – 272 – 3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571 – 272 - 3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Pramila Parthasarathy  
October 25, 2004.

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100